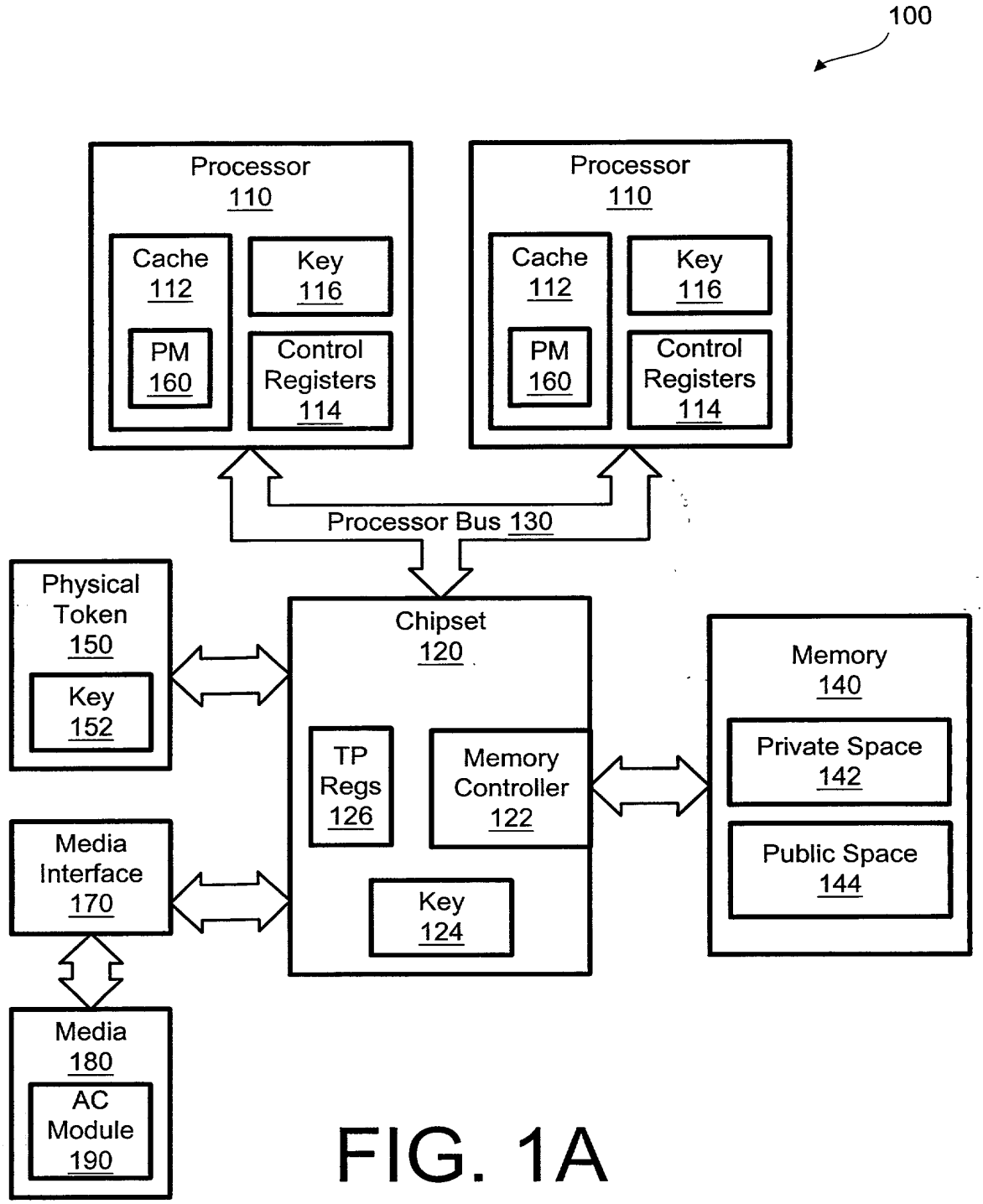
100
Processor
110
Cache
112
Key
116
PM
160
Control
Registers
114
Processor
110
Cache
112
Key
116
PM
160
Control
Registers
114
Processor Bus 130
Physical
Token
150
Key
152
Chipset
120
TP
Regs
126
Memory
Controller
122
Key
124
Memory
140
Private Space
142
Public Space
144
Media
Interface
170
Media
180
AC
Module
190

FIG. 1A

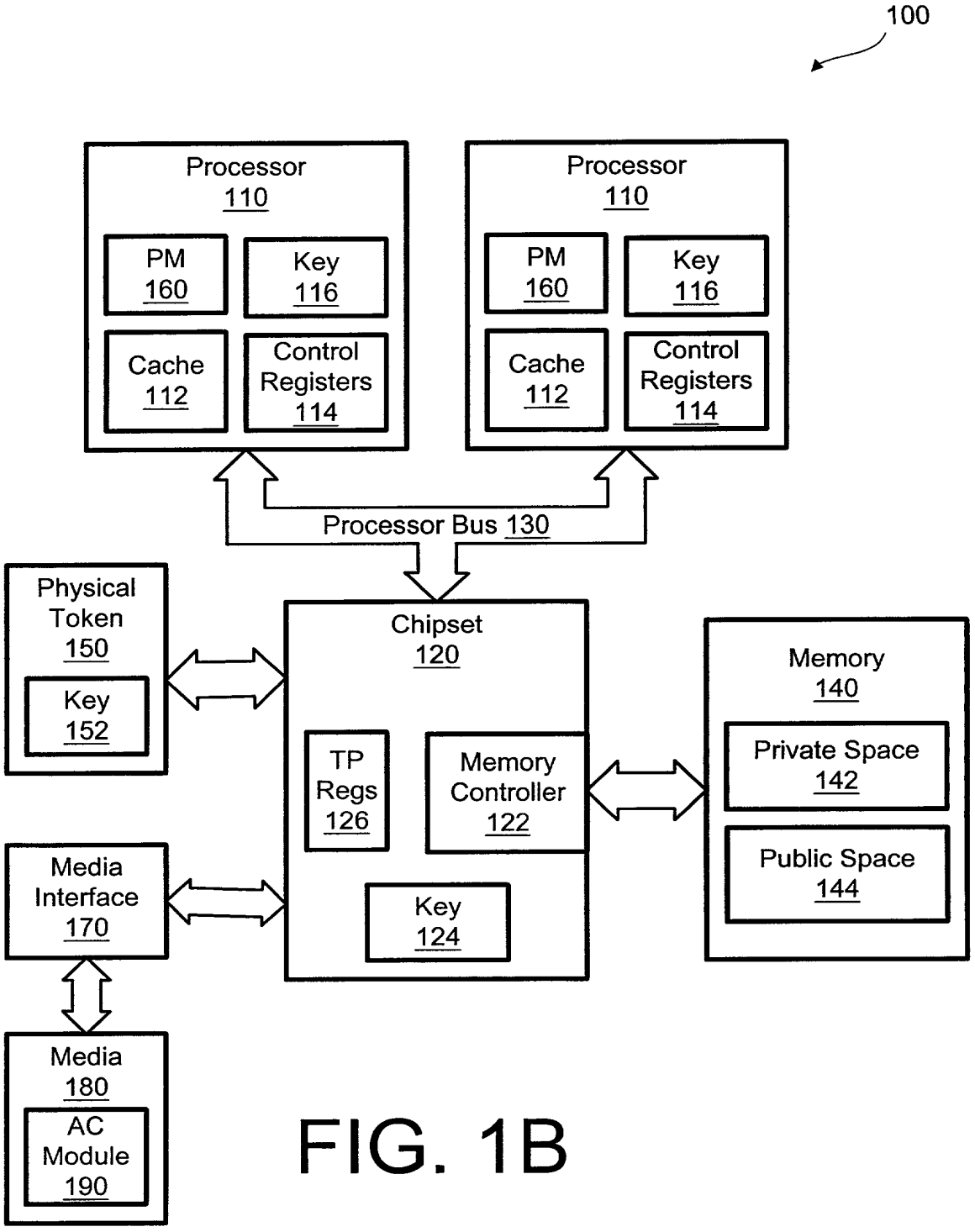
100
Processor
110
PM
160
Key
116
Cache
112
Control
Registers
114
Processor
110
PM
160
Key
116
Cache
112
Control
Registers
114
Processor Bus 130
Physical
Token
150
Key
152
Chipset
120
TP
Regs
126
Memory
Controller
122
Key
124
Memory
140
Private Space
142
Public Space
144
Media
Interface
170
Media
180
AC
Module
190

FIG. 1B

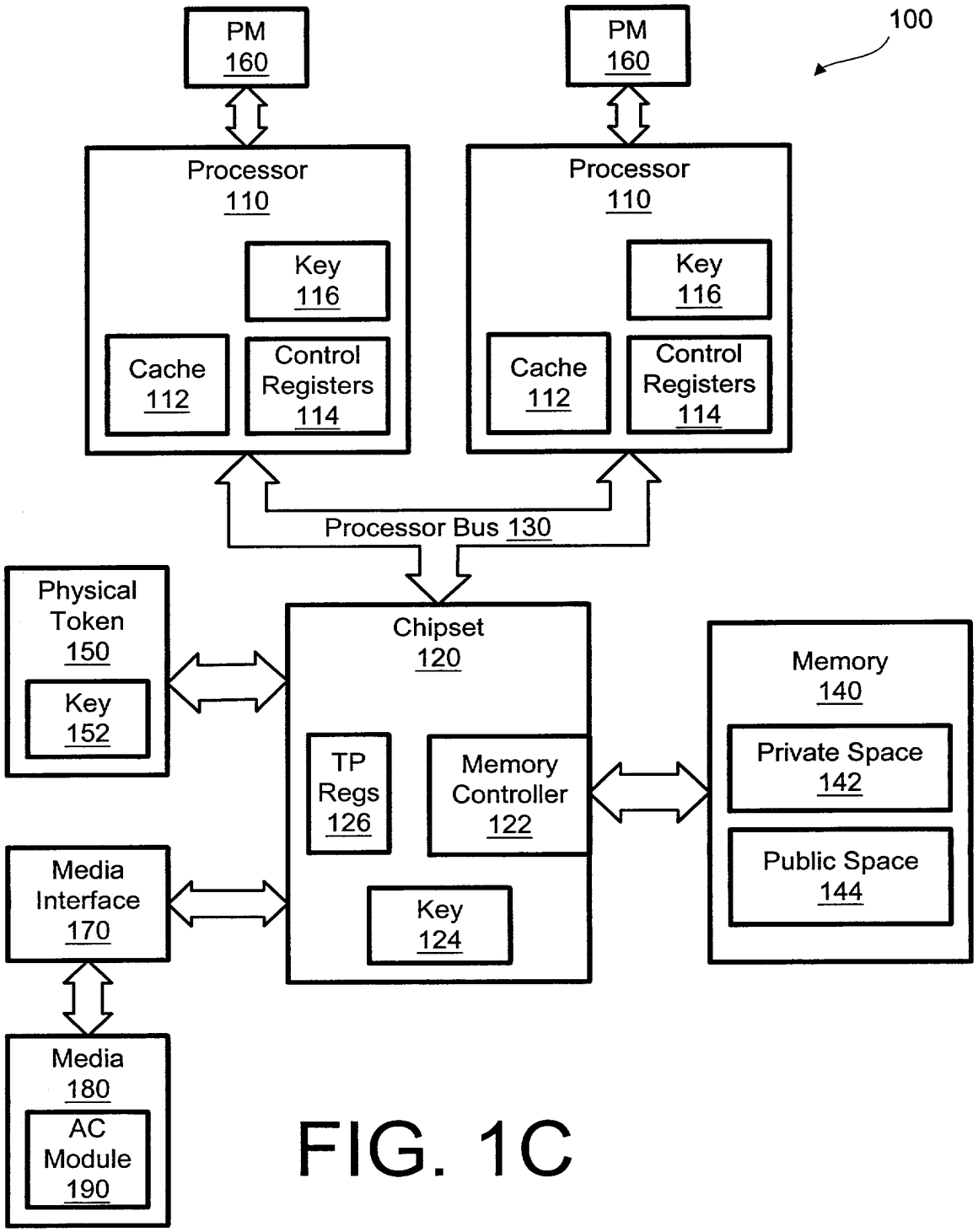
100
PM
160
PM
160
Processor
110
Processor
110
Key
116
Key
116
Cache
112
Control
Registers
114
Cache
112
Control
Registers
114
Processor Bus 130
Physical
Token
150
Key
152
Chipset
120
TP
Regs
126
Memory
Controller
122
Key
124
Memory
140
Private Space
142
Public Space
144
Media
Interface
170
Media
180
AC
Module
190

FIG. 1C

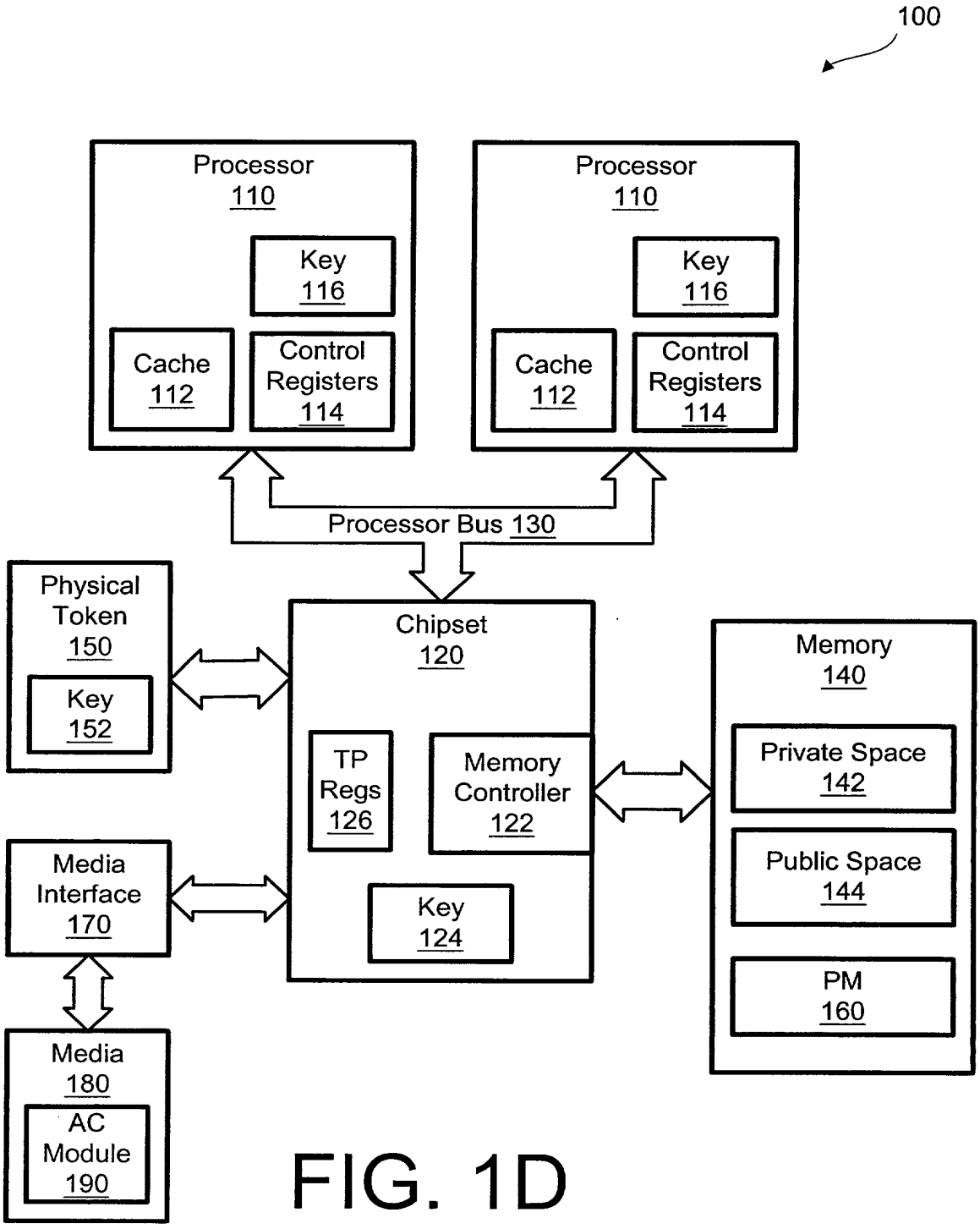
100
Processor
110
Key
116
Cache
112
Control
Registers
114
Processor
110
Key
116
Cache
112
Control
Registers
114
Processor Bus 130
Physical
Token
150
Key
152
Chipset
120
TP
Regs
126
Memory
Controller
122
Key
124
Memory
140
Private Space
142
Public Space
144
PM
160
Media
Interface
170
Media
180
AC
Module
190

FIG. 1D

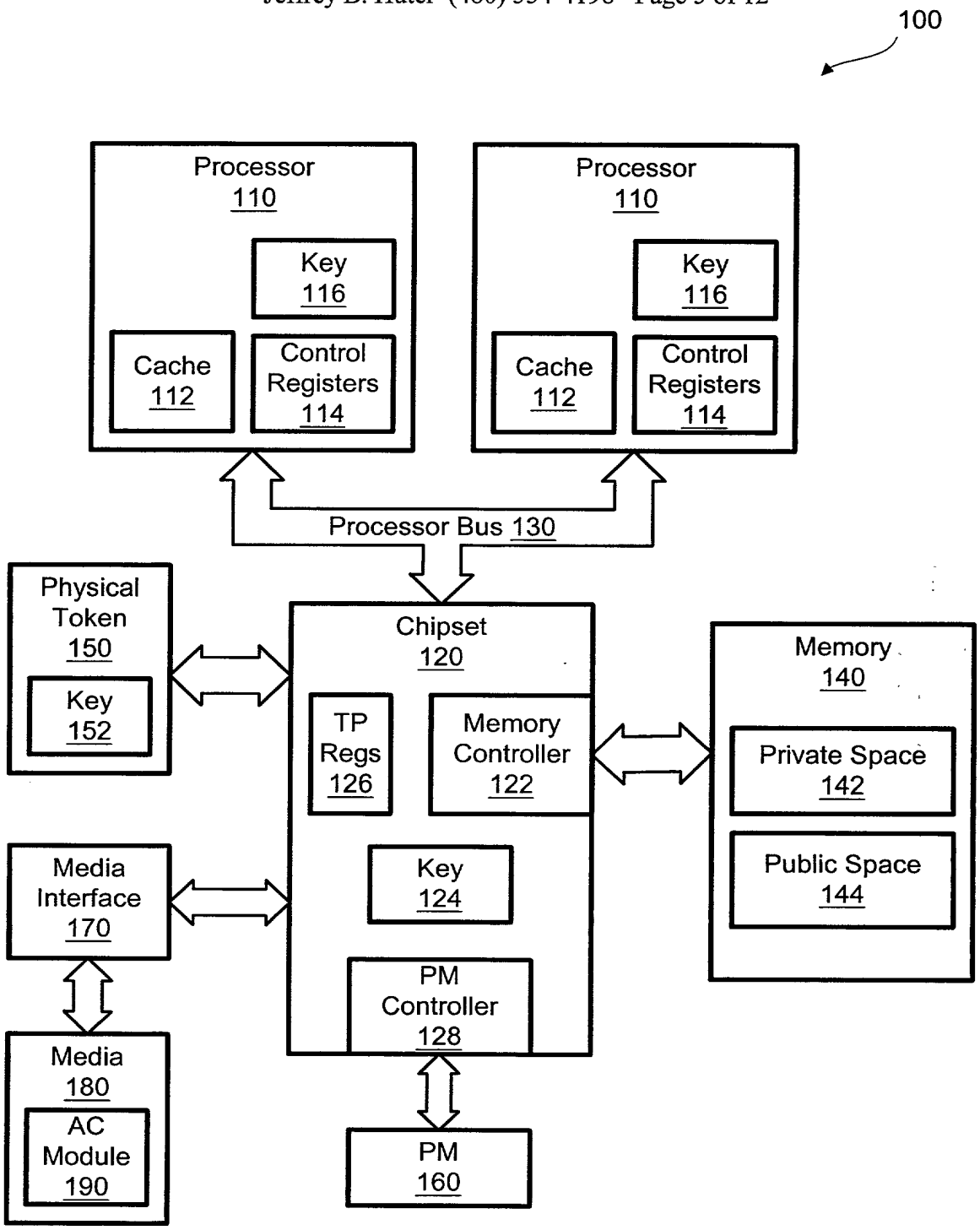
100
Processor
110
Key
116
Cache
112
Control
Registers
114
Processor
110
Key
116
Cache
112
Control
Registers
114
Processor Bus 130
Physical
Token
150
Key
152
Chipset
120
TP
Regs
126
Memory
Controller
122
Key
124
PM
Controller
128
Memory
140
Private Space
142
Public Space
144
Media
Interface
170
Media
180
AC
Module
190
PM
160

FIG. 1E

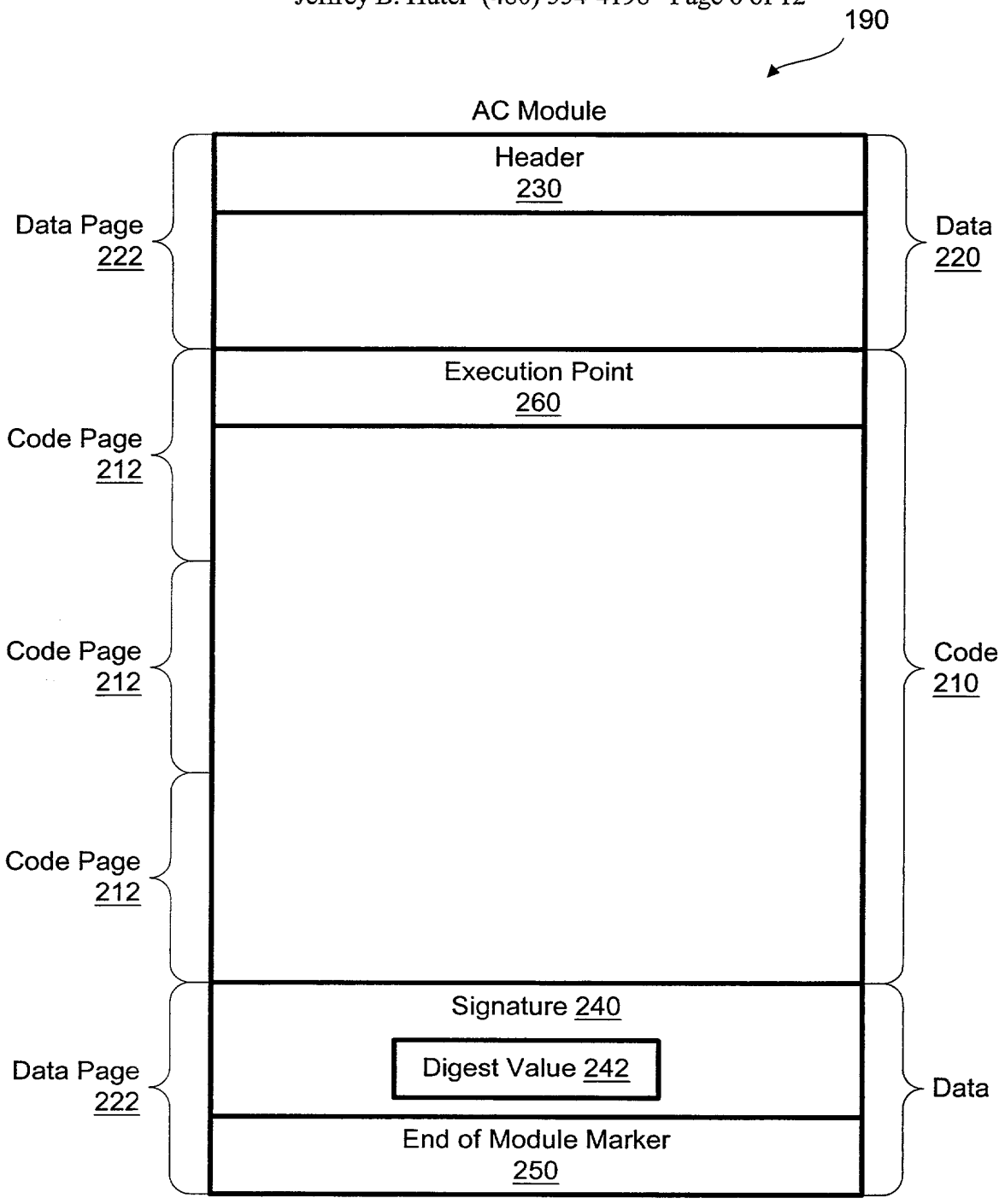
190
AC Module
Header
230
Data Page
222
Data
220
Execution Point
260
Code Page
212
Code Page
212
Code
210
Code Page
212
Signature 240
Digest Value 242
Data Page
222
Data
End of Module Marker
250

FIG. 2

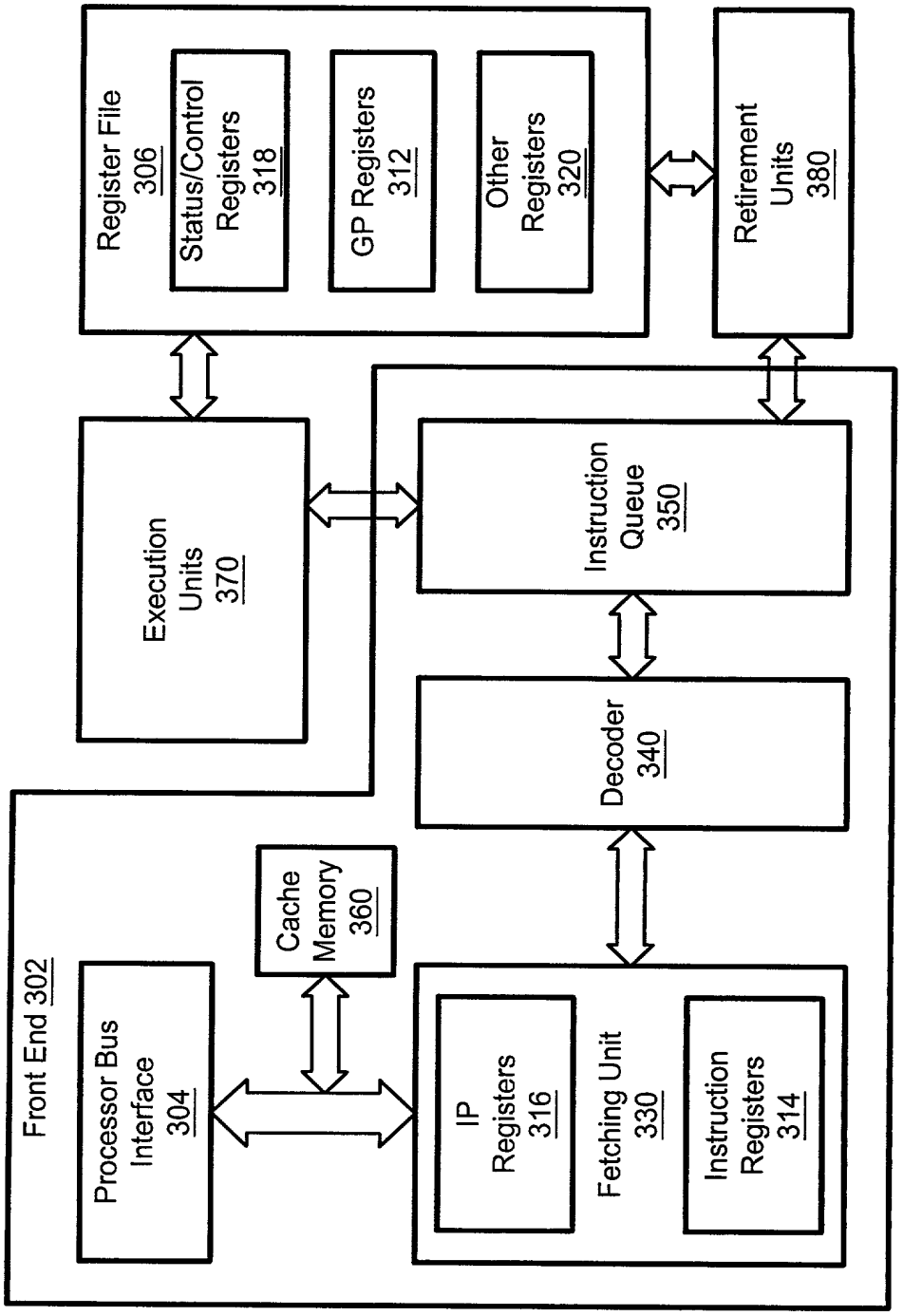
Register File 306
Status/Control Registers 318
GP Registers 312
Other Registers 320
Retirement Units 380
Execution Units 370
Instruction Queue 350
Decoder 340
Cache Memory 360
Front End 302
Processor Bus Interface 304
IP Registers 316
Fetching Unit 330
Instruction Registers 314

FIG. 3

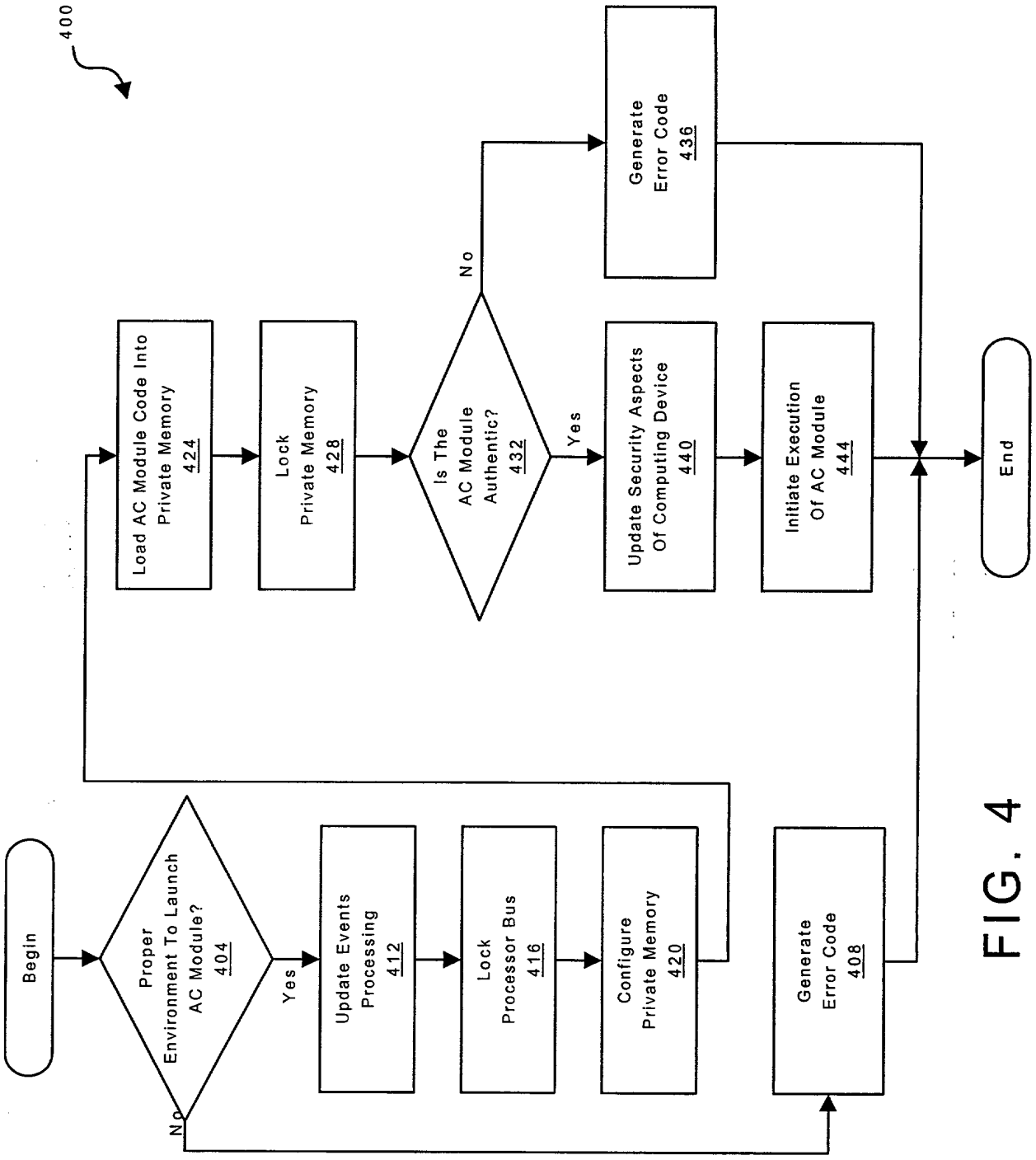
400
Begin
Proper Environment To Launch AC Module? 404
No
Yes
Update Events Processing 412
Lock Processor Bus 416
Configure Private Memory 420
Generate Error Code 408
Load AC Module Code Into Private Memory 424
Lock Private Memory 428
Is The AC Module Authentic? 432
No
Yes
Generate Error Code 436
Update Security Aspects Of Computing Device 440
Initiate Execution Of AC Module 444
End

FIG. 4

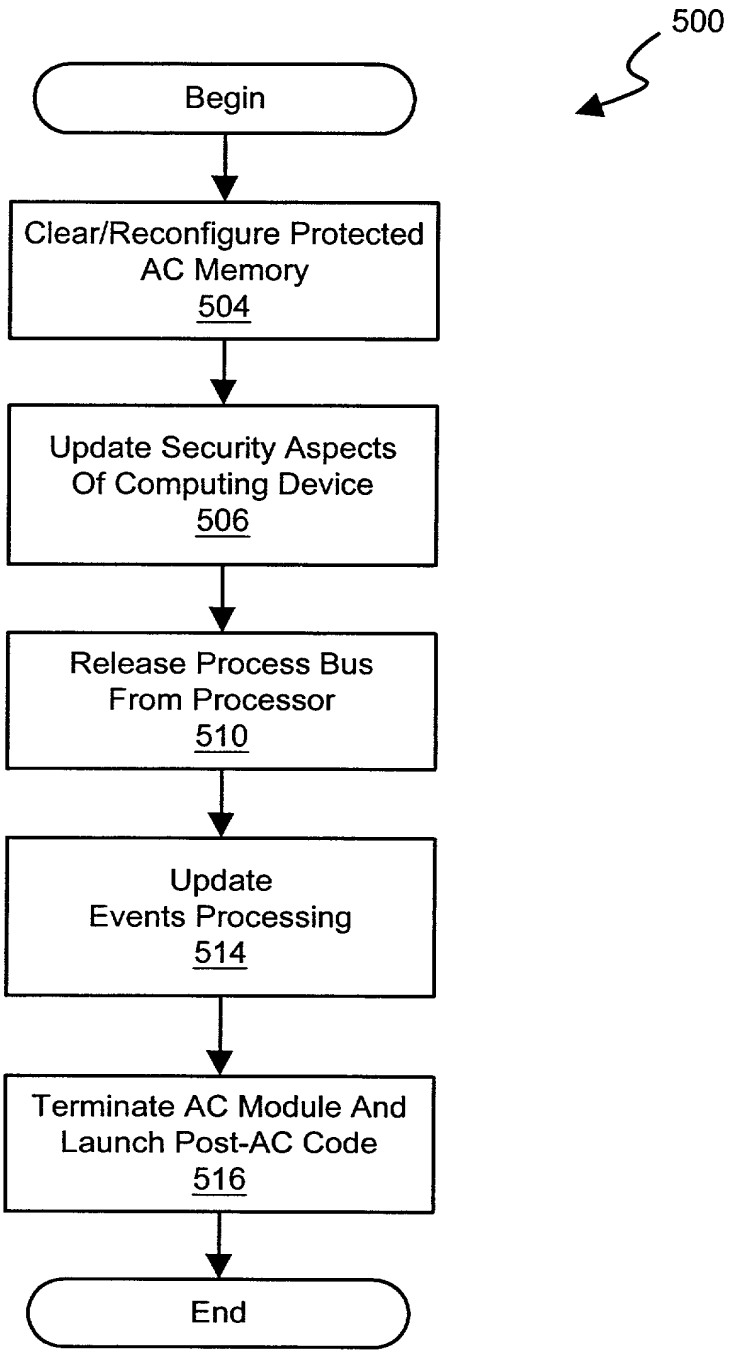
500
Begin
Clear/Reconfigure Protected AC Memory
504
Update Security Aspects Of Computing Device
506
Release Process Bus From Processor
510
Update Events Processing
514
Terminate AC Module And Launch Post-AC Code
516
End

FIG. 5

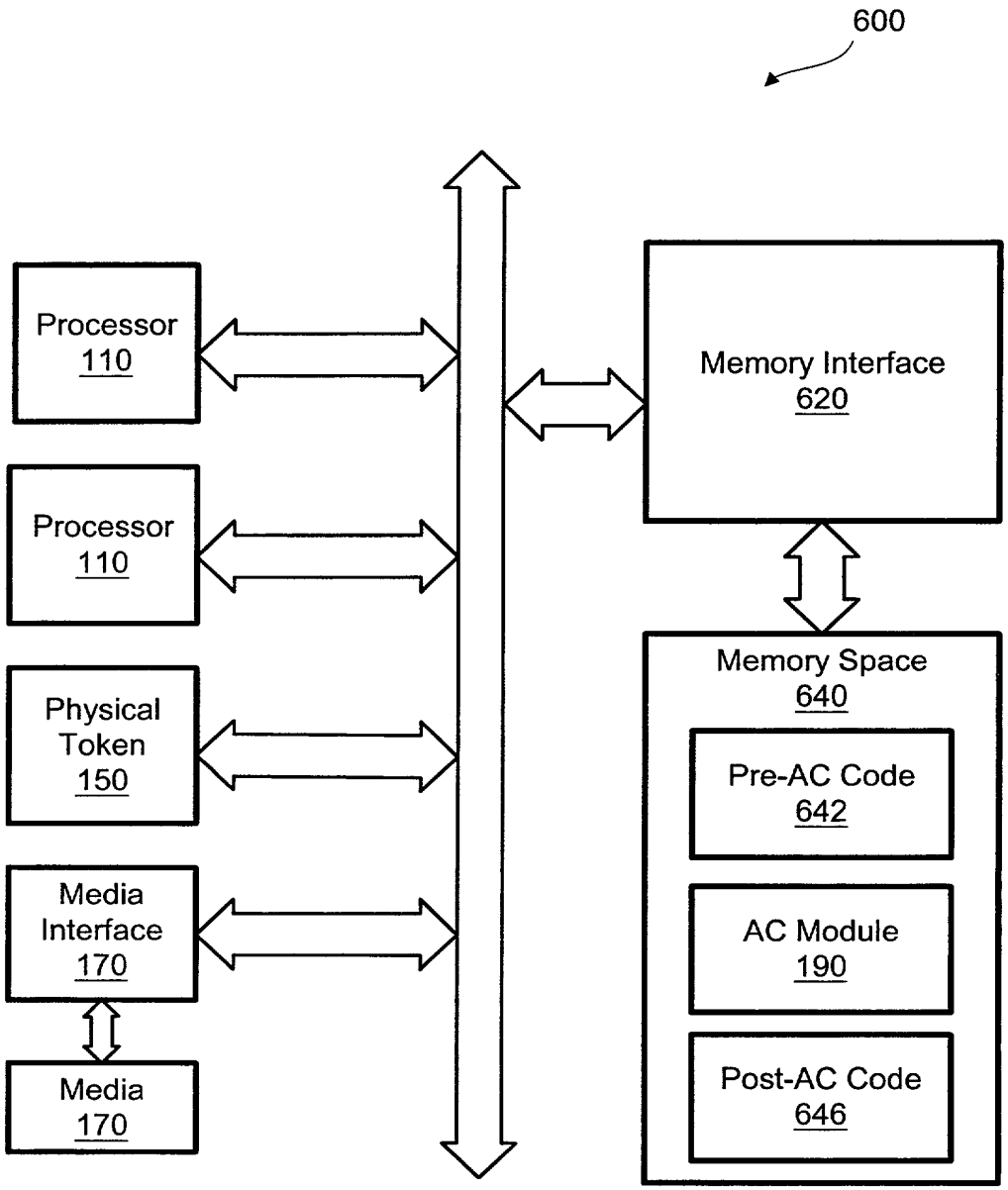
600
Processor
110
Processor
110
Physical
Token
150
Media
Interface
170
Media
170
Memory Interface
620
Memory Space
640
Pre-AC Code
642
AC Module
190
Post-AC Code
646

FIG. 6

Document: 42390p13769

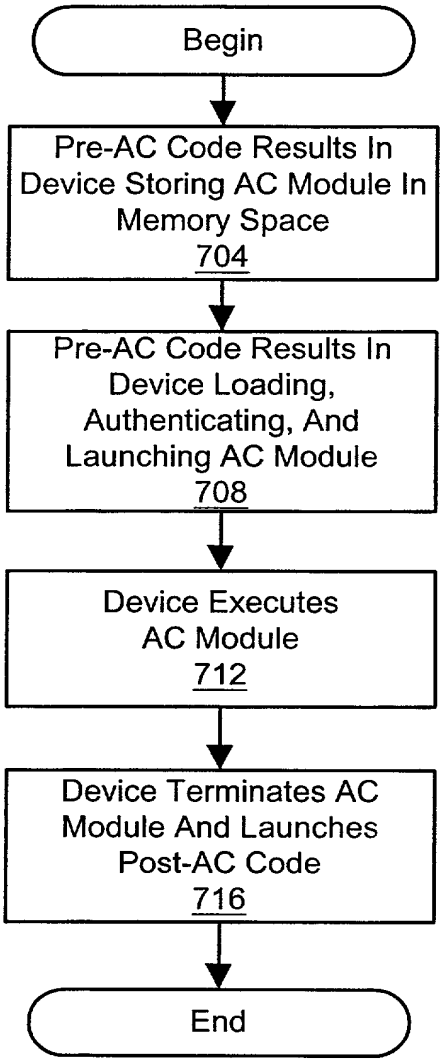

FIG. 7A

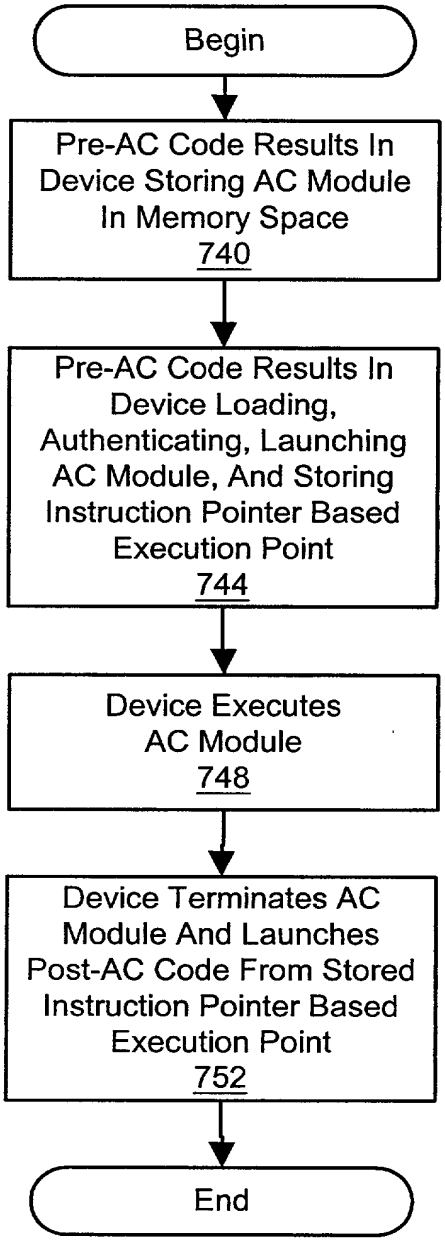

FIG. 7B

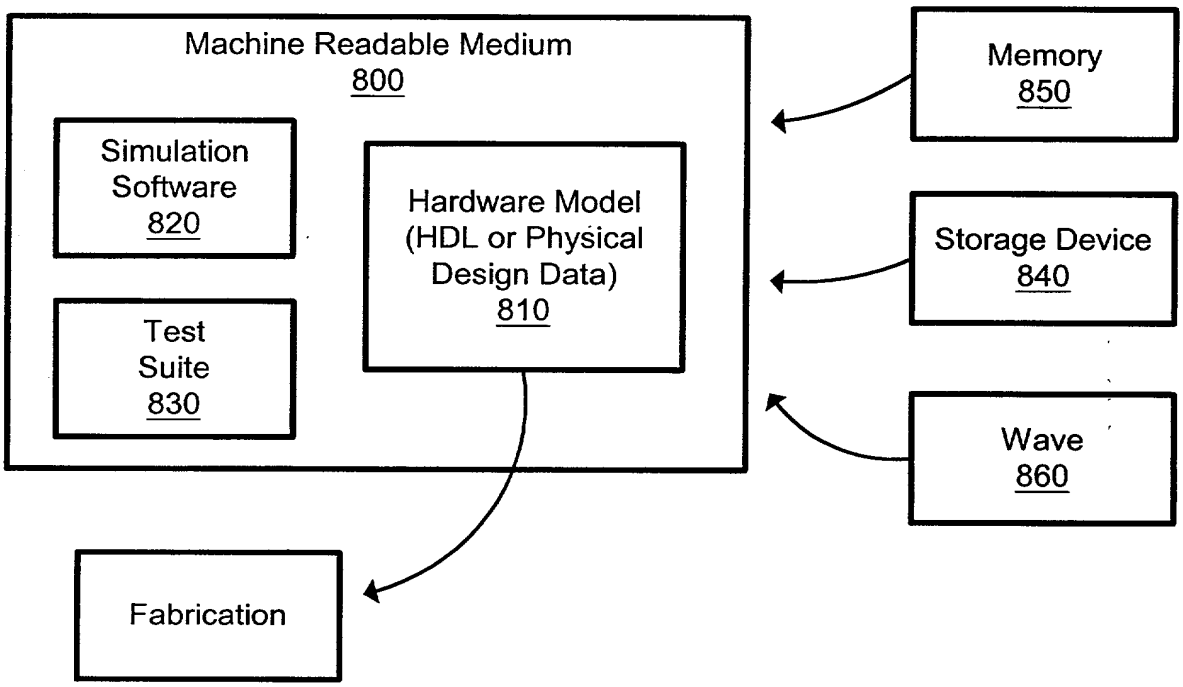
Machine Readable Medium
800
Simulation Software
820
Hardware Model (HDL or Physical Design Data)
810
Test Suite
830
Fabrication
Memory
850
Storage Device
840
Wave
860

FIG. 8